

WEBSense CLIENT POLICY MANAGER



WebSense® Client Policy Manager™ (CPM) provides a comprehensive endpoint security solution for desktops, laptops, and servers that proactively protects organizations against known and unknown security threats.

CPM prevents the installation and execution of unauthorized applications and enforces application use policies with its comprehensive database of categorized applications, which is updated daily. With application control, CPM provides an easy-to-implement, low risk, and highly effective alternative to cumbersome behavior-based Host Intrusion Prevention Systems (HIPS). The comprehensive coverage of both “whitelist” (good) and “blacklist” (bad) applications allows for granular, dynamic, and highly flexible application policies. CPM complements desktop antivirus and personal firewalls while stopping today’s fast-moving and blended security threats.

Prevent Attacks

CPM provides an immediate “first line of defense”—security starts and stops at the endpoint.

- Provides application awareness and usage policy enforcement on the endpoint for blocking malicious software while ensuring compliance and productivity.
- Prevents malicious applications from changing registry settings and tracks suspicious registry activities.
- Protects remote and mobile users operating outside of the network or without standard security updates or patches.
- Includes protection from threats and compliance risks around web access and URL content for remote and mobile users.
- Works with Network Access Control (NAC) solutions to enforce policy on devices trying to enter the network, denying access to non-compliant endpoints.
- Via integrations, enables network-level protection from inbound threats and creates dynamic and application-aware firewalling.
- Provides multiple levels of control to prevent the launch or mitigate the propagation of security attacks:
 - Provides maximum control over endpoints by allowing only approved applications to run, preventing potentially malicious and unwanted applications from launching.
 - Blocks application network access to specific ports and protocols by application category, preventing the propagation of malicious software or unauthorized outbound communications.
 - Allows system administrators to preempt attacks and vulnerabilities by immediately securing endpoint configurations to stop the execution of any new software that may be inappropriate, harmful, or seeking to exploit newly published operating system or application vulnerabilities.

Control Desktop Application Use

CPM proactively monitors user application inventories and activity, and reduces Help Desk calls associated with unauthorized application use:

- Enforces flexible, auto-updating application use policies to protect end users from malicious and potentially unwanted software.
- Prevents the installation and execution of unauthorized applications.

CPM includes advanced reporting tools which help:

- Determine the organization's risk profile.
- Detect the presence and location of malicious mobile code (MMC), spyware, hacking tools, or other security risks on each machine and server.
- Perform critical software assessments that provide categorized and normalized views of programs and applications.
- Enable early threat detection and identification of potential application vulnerabilities.

Safeguard Information

CPM provides another layer of control over data at the endpoint by blocking the potential theft of private information or intellectual property via removable media or network communications:

- Allows system administrators to prevent devices such as flash drives, CD/DVD burners, floppy drives, and external hard drives from being used on client workstations, minimizing the risk of introducing malicious software to the organization. Organizations can also block writable media, depending upon their policies.

Streamline Operations

CPM reduces the level of effort to deploy and manage an endpoint security solution:

- Integrates with leading directory services for creating user- and group-based policies.
- Integrates with Windows® Firewall in Microsoft® Windows XP Service Pack 2 (SP2) to simplify firewall management and automate program exceptions through awareness of application and port content.

Extend Protection to Remote and Mobile Users

CPM's Remote Filtering capabilities allow organizations to apply their same Websense Enterprise® or Websense Web Security Suite™ web filtering policies to remote office and mobile laptop users outside of the network to protect them from malicious and inappropriate websites.

CPM: Powered by Innovative Websense ThreatSeeker™ Technology

Websense ThreatSeeker technology delivers preemptive protection from web-based security threats—threats typically missed or too costly to prevent using traditional security technologies. Unlike these approaches, Websense seeks out threats on the internet before customers are compromised and protects customers before patches and signatures are created.

Websense ThreatSeeker uses more than 100 proprietary processes and systems to decipher emerging and complex threats and runs using a combination of mathematical algorithms, behavior profiling, code analysis, as well as an extensive network of data mining machines. The foundation of all Websense security software products, Websense ThreatSeeker provides ongoing threat intelligence and delivers automatic protection to customers within minutes.

The Websense Web Security Ecosystem™

The Websense Web Security Ecosystem is a comprehensive framework of technology integrations that provides enhanced security and ease of deployment of Websense web security solutions in enterprise environments. The Websense Web Security Ecosystem incorporates world-class security and networking technologies including: internet gateways, network access control, security event management, identity management, and appliance platforms. Through seamless integration with more than 40 different technology solutions, the Websense Web Security Ecosystem helps organizations identify and mitigate web-based threats and vulnerabilities.

System Requirements

Client Policy Manager Server

- Microsoft Windows Server® 2003 Standard Edition or Enterprise Edition, or the same with SP1
- Microsoft Windows 2000 Server with SP3 or higher

Client Policy Manager and Remote Filtering Clients

- Microsoft Windows XP Professional with SP1 or SP2
- Microsoft Windows Server 2003 Standard Edition or Enterprise Edition with SP1
- Microsoft Windows 2000 Professional, Server, or Advanced Server with SP3 or SP4

Remote Filtering Server

- Microsoft Windows Server 2003 Standard Edition or Enterprise Edition, or the same with SP1
- Microsoft Windows 2000 Server with SP3 or higher
- Red Hat® Enterprise Linux® 3 or 4: AS, ES, or WS, or Red Hat Linux 9
- Sun® Solaris™ 9 or 10

Summary

CPM protects computers both inside and outside of the corporate network by detecting and analyzing endpoint security threats and application activity, and by enforcing flexible, scalable, auto-updating application use policies. Integrating seamlessly with existing IT infrastructures, CPM protects all users against known and unknown security threats.

WebSense, Inc.

San Diego, CA USA
tel 800 723 1166
tel 858 320 8000
www.websense.com

Australia
websense.com.au

Brazil
portuguese.websense.com

Colombia
websense.com.es

France
websense.fr

Germany
websense.de

Hong Kong
websense.cn

India
websense.com

Ireland
websense.ie

WebSense UK Ltd.

Chertsey, Surrey UK
tel +44 (0) 1932 796300
fax +44 (0) 1932 796601
www.websense.co.uk

Italy
websense.it

Japan
websense.jp

Mexico
websense.com.es

PRC
prc.websense.com

Spain
websense.com.es

Sweden
websense.com

Taiwan
websense.cn

Download a free 30-day evaluation today www.websense.com/downloads

